Accellion Share Securely™

AN ACCELLION WHITE PAPER

Mobilize SharePoint Securely: Top 5 Enterprise Requirements

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

WP-5SPREQS1112

Executive Summary

To stay productive, mobile users want continuous access to business data—including data stored in Enterprise Content Management (ECM) systems such as Microsoft® SharePoint – and they want to collaborate on and share that information with co-workers, business partners, vendors and customers. When they discover how difficult it is to access SharePoint files on smartphones and tablets, they often do an end run around corporate IT and post files to cloud-based file-sharing services like Dropbox. Copies of SharePoint files then spread from device to device, unmonitored and uncontrolled by IT.

Dropbox and other consumer file sharing services can pose significant security and compliance risks to enterprises. They cannot be centrally controlled or monitored by IT administrators. They also lack the rigorous security features, such as encryption and auditable log files, that enterprises need in order to keep data safe and to demonstrate compliance with industry regulations such as HIPAA and Sarbanes-Oxley (SOX).

Enterprise IT departments need to step in, take charge, and mobilize SharePoint securely. By deploying a SharePoint-enabled secure mobility solution, IT can fully leverage the corporate investment in SharePoint while keeping mobile workers productive and focused on core business needs.

To mobilize SharePoint securely, enterprises should look for a solution that meets these five requirements:

1. Provides secure access to SharePoint and other ECM systems.
2. Unites disparate content silos.
3. Supports secure collaboration between internal and external users.
4. Secures content and centralizes IT management and control.
5. Enables compliance with industry regulations.

The Changing Enterprise IT Landscape

In the past few years, the enterprise IT landscape has changed dramatically. More services are cloud-based. And nearly every organization has gone mobile. Mobile workers now comprise the majority of the U.S. workforce, and those workers are usually carrying devices, such as iOS and Android phones and tablets, which they have purchased themselves.

Not all of these changes have been harmonious. In particular, the growth of mobile computing has created new IT challenges for enterprises that have invested heavily in ECM systems, in particular SharePoint.

Let's explore these IT trends and the challenges they create for enterprises today.

A Deep Investment in ECM

Businesses continue to deepen their commitment to ECM systems and to SharePoint in particular. Over 17,000 organizations[1] now run SharePoint. Among enterprise sites running SharePoint, 67% have rolled out SharePoint for all their users. These site-wide deployments have helped Microsoft sell millions of SharePoint licenses—125 million licenses to date.[2] Across the board, private- and public-sector organizations have adopted SharePoint as the system of choice for storing and internally sharing the documents that power their organization.

The BYOD Revolution

While enterprises have been investing in SharePoint and other ECM systems, their employees have been investing in smartphones such, as iPhones and Android phones, and tablets, such as iPads and Samsung Galaxy Notes. Over 90% of U.S. businesses[3] now support some form of a Bring Your Own Device (BYOD) policy, allowing users to bring their own smartphones and tablets to work. This has had a dramatic impact on IT. Instead of provisioning a homogenous environment of servers and desktop systems running Windows operating systems, IT departments are now tasked with managing wildly varied environments comprising in-house servers, third-party cloud services, and an ever-changing mixture of desktops, laptops, smart phones, and tablets running different operating systems.

The BYOD revolution doesn't simply replace last year's desktop system with a single mobile device. Instead it multiplies the number of devices and platforms that each employee is using. On average, mobile workers are carrying 2.8 mobile devices today, and they'll likely carry three or more devices by 2014.[4] The challenge for organizations is supporting users who want consistent access to enterprise content on all their devices.

Mobile workers want all their devices to be able to access all the files they need for work. And all devices should present a consistent, up-to-the-minute view of those files, so that employees don't end up working on the wrong version of a file simply because they picked up one device instead of another. Desktops, laptops, smartphones, and tablets should all be able to access the same versions of the same files. The sales proposal presented on a table should include the edits entered moments earlier on a smartphone. In order to effectively address this expectation, there needs to be a shared access to the "document of record," typically the one stored in SharePoint.

[1] http://www.microsoft.com/en-us/news/exec/kurtd/10-03-11sharepoint.aspx
[2] http://www.zdnet.com/blog/microsoft/whats-keeping-the-microsoft-beancounters-awake-at-night/8632
[3] http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD
[4] http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD

In the classic IT-centric model, a user would use VPN software to "tunnel" into the corporate network from a laptop or desktop computer, browse the SharePoint universe to find the document they need, perform whatever functions they needed to on the document (edit, e-mail, print, comment on, etc.), and then save it back to SharePoint. This does not work effectively or consistently in the BYOD universe, especially when users want to use their personal, non-IT issued devices.

Rather than working with the document of record stored in SharePoint, they're selecting external cloud-based services to propagate copies of SharePoint files to their own devices and to the devices of colleagues, clients and partners.

The Risky Result: Ad Hoc File Sharing

There is no shortage of file-sharing services available to users interested in going mobile. Free file-sharing services such as Dropbox automatically copy and synchronize copies of files across multiple devices. Users simply install Dropbox clients on their desktops and on all their mobile devices, and presto! Business files are copied everywhere automatically. Need to share files with external users? No problem. Simply invite them to access the folders you want to share.

Problem solved? Not at all. File-sharing services, such as Dropbox, create a whole new set of security and compliance problems for enterprise organizations.

Lack of Monitoring and Control

Free file sharing services leave IT administrators with no way of monitoring or controlling the distribution of files through these services. IT has no easy way of even discovering which users have signed up for these services, nor do they have any way of monitoring which files are being distributed and to whom. The reality is, in most enterprises today, confidential information - customer records, product designs, sales projections, HR records, and patent applications – is synced through public cloud services across multiple devices belonging to any number of users. IT simply has to hope that this unmonitored, uncontrolled, and ad hoc distribution of data doesn't leak confidential data, expose company secrets or other intellectual property, and trigger any lawsuits or compliance violations.

Most organizations would probably be shocked to discover just how far-flung confidential data really is. IBM recently discovered[5] product plans and other confidential files had been posted to unauthorized locations on the Internet. To stanch data leaks such as these, the company has banned Apple iCloud, Dropbox, Evernote, and other popular file-syncing services from its network and its employees' devices.[6]

Need for Security

Free file-sharing services lack the rigorous security features that enterprises require. In addition to providing monitoring and access control features, enterprise file sharing requires the ability to be able to encrypt files at rest and in transit so that data confidentiality is never breached. Free file-sharing services are fine for sharing less sensitive files such as family photos. But customer records with credit card data or Social Security Numbers should always be encrypted to keep the data safe. This is not only a best practice; it's the law in many industries and in states such as Massachusetts and Nevada.

Beyond these security features, free file sharing services have proven vulnerable to failure. Dropbox accidentally turned off all password protection for all accounts for four hours. To this

[5] http://www.computerworld.com/s/article/9228147/BYOD_exposes_the_perils_of_cloud_storage
[6] http://blogs.wsj.com/cio/2012/05/22/if-ibm-finds-byod-a-challenge/

day, the company is unable to provide an accounting of which users accessed which files during that time. The company has suffered other data breaches as well, including the breach of an employee's account that led to Dropbox users being deluged with spam.[7]

One More Twist: Disparate Content Silos

Even in organizations that have rolled out SharePoint access to all users, not all business information resides in SharePoint. It resides in databases, in application-specific content management systems, on network servers and in a diffuse collection of end-user devices.

The lack of a universal data repository only encourages users to create their own lowest common denominator for file management and file-syncing. Employees copy the files they need not only from SharePoint but from other content silos and collect them in easily accessible, free, cloud file sharing services, where they are, in turn, synced to multiple devices and potentially multiple user accounts.

The bottom line? Ad hoc file sharing and file syncing doesn't just undermine the security features of SharePoint. It's a bigger problem that affects every content source in the enterprise, and compounds the security and IT challenge of providing an effective, business-friendly solution.

The Enterprise IT Response

To protect confidential data, prevent the loss of intellectual capital, and avoid regulatory penalties for compliance failures, enterprise IT organizations need to find a solution that makes SharePoint (and other enterprise content) securely available to authorized mobile users. The solution should be so easy to use that employees aren't tempted to find dangerous work-arounds. As part of its implementation of a secure mobile access solution, IT should block risky services like Dropbox, ensuring that mobile file sharing and access always take place through services that can be monitored and controlled by IT. The solution should improve security while giving employees the fast, easy, and secure data access they need.

Key Requirements to Mobilize SharePoint Securely

Here are five requirements for an enterprise-class solution that meets line-of-business and IT objectives.

1. Mobile Access to SharePoint without VPNs

The secure mobile access solution should make it easy for authorized users to access the files they need on SharePoint without relying on VPNs. Users should be able to access SharePoint files directly without having to first copy those files elsewhere.

2. Unified Access to Disparate Content Silos

Providing secure mobile access to SharePoint is a critical first step; unifying the user experience so they can easily access all relevant SharePoint content is essential. If users lack secure mobile access to other ECM systems and file servers, they still might be tempted to use risky, cloud based file sharing services. Enterprises should deploy a secure mobile access solution that integrates with all leading ECM systems, industry standard file services such as NFS, and the local file system of the device in use.

[7] http://bits.blogs.nytimes.com/2012/08/01/dropbox-spam-attack-tied-to-stolen-employee-password/

3. Collaboration with Internal and External Users

Business often requires that employees collaborate with external users, such as business partners, consultants, and even customers. As workforces become more global and distributed, cross-boundary collaboration among teams of specialists is becoming increasingly common. This is, paradoxically, one of the reasons why workers turn to non-IT administered file sharing systems for day-to-day document access. IT tools for collaboration and file-sharing must support convenient but secure file-sharing among internal and external users. IT organizations understand how important this flexibility is for enabling employees to get work done—in a recent survey of enterprise IT managers,[8] the vast majority (86%) rated the ability to collaborate with both internal and external users as critical or very important. While there are solid financial, security and administrative reasons why those users should never be allowed direct access to content inside the firewall; the mobile access solution for SharePoint should support file sharing between all types of authorized users, both internal and external.

4. Comprehensive Security, Centralized Oversight and Control

The secure mobile access solution should provide industry-leading security features, such as strict access controls, defense against brute-force password attacks, and rigorous encryption of data in transit and at rest. IT administrators should have fine-grained control over which users have access to which files. If an employee leaves the organization, IT should be able to immediately disable access to confidential files, even if those files reside on mobile devices.

5. Support for Compliance with Data Privacy and Security Laws and Regulations

To comply with industry regulations such as HIPAA and SOX, enterprises must implement features beyond access controls and encryption. They also need to implement logging and auditing, so that the organization always keeps control of sensitive confidential information and IT administrators and compliance officers can monitor user activity and ensure it complies with policies and regulations. A secure mobile access solution should support these additional capabilities to ensure that mobile access never jeopardizes compliance.

Conclusion

Microsoft SharePoint and other ECM systems provide rich collaborative workspaces and data storage solutions for enterprises. By mobilizing SharePoint and ECM systems securely, enterprises can maximize productivity and fully leverage their existing enterprise investments while ensuring that business data is always safe.

For information about Accellion's solution to mobilize SharePoint securely, please visit www.accellion.com.

[8] IDG Research finding quoted in "The Cloud: Reinventing Enterprise Collaboration," a white paper published by *CSO Magazine* and *CIO Magazine*.